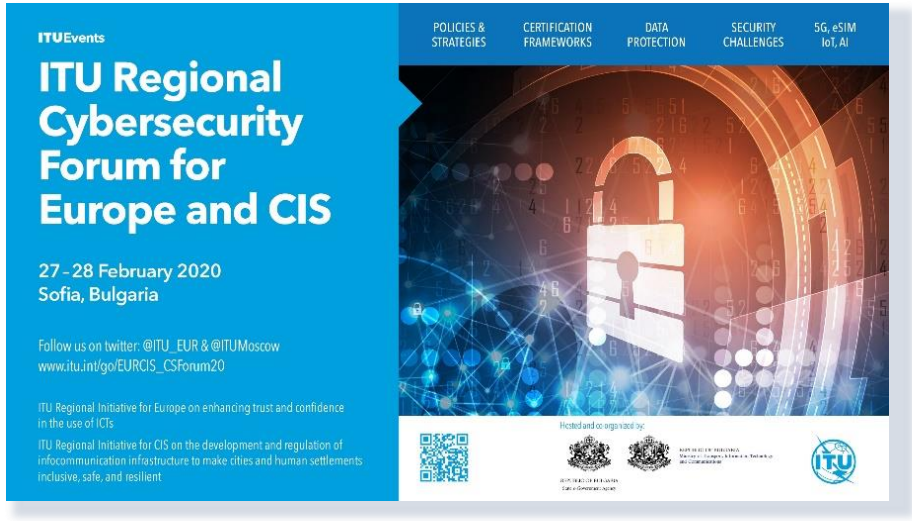
Состояние кибербезопасности Узбекистана

Гафуров Шарифжон Рахимович
ГУП «Центр кибербезопасности»
февраль 2020, София



Нормативно-правовое регулирование

- Закон Республики Узбекистан «Об информатизации»
- Закон Республики Узбекистан «Об электронном правительстве»
- Закон Республики Узбекистан «О защите информации в автоматизированной банковской системе»
- Указ Президента Республики Узбекистан №УП-4947 от 7.02.2017 года «О стратегии действий по дальнейшему развитию Республики Узбекистан»
- Постановление Президента Республики Узбекистан №ПП-4024 от 21.11.2018 «О мерах по совершенствованию системы контроля за внедрением информационных технологий и коммуникаций, организации их защиты»
- Постановление Президента Республики Узбекистан №ПП-4452 от 14.09.2019 «О дополнительных мерах по совершенствованию системы контроля за внедрением информационных технологий и коммуникаций, организации их защиты»

Организационные и технические меры

разработка, рассмотрение и согласование Политики информационной безопасности

консультационная помощь государственным и хозяйственным органам
по организационным и техническим вопросам обеспечения информационной и
кибербезопасности

предоставление государственным и хозяйственным органам нормативных актов
в области обеспечения информационной и кибербезопасности (нормативное
обеспечение)

проведение семинаров и тренингов по вопросам обеспечения информационной
и кибербезопасности

согласование ежегодных планов мероприятий по обеспечению
информационной и кибербезопасности государственных и хозяйственных
органов, координация их исполнения

Организационные и технические меры

Ведется круглосуточное мониторинг

Система оповещений и предотвращений проникновения к информационным ресурсам (веб-сайтам)

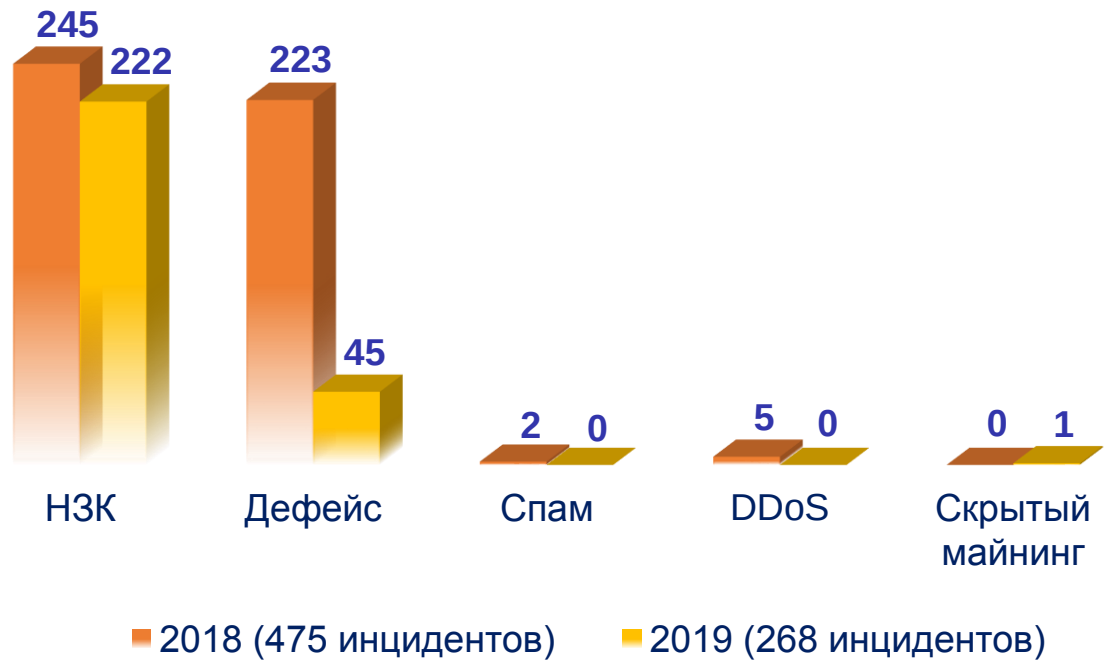
Система обнаружения инцидентов на информационных ресурсах доменной зоны. «UZ»

Система мониторинга событий информационной безопасности в межведомственной сети передачи данных

Инциденты кибербезопасности

Выявленные инциденты кибербезопасности в национальном сегменте сети интернет

Инциденты кибербезопасности выявленные в национальном сегменте сети интернет за 2018 и 2019 года



Угрозы кибербезопасности

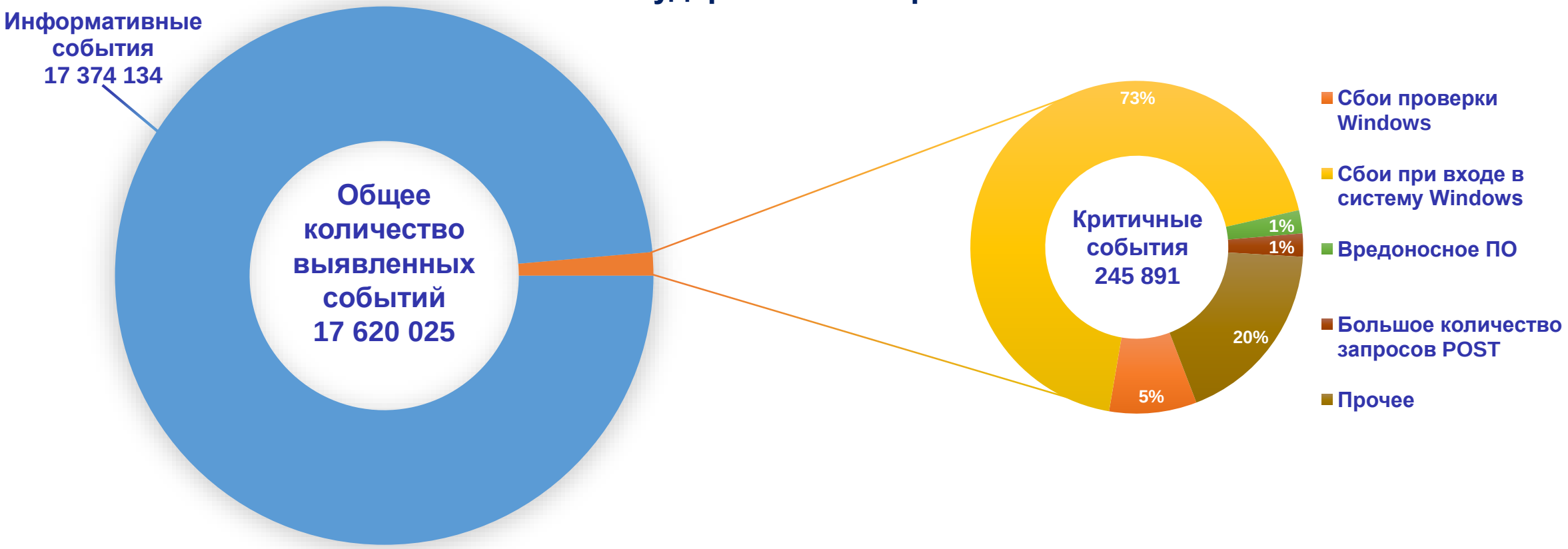
Выявленные уязвимости в информационных системах и веб-сайтах

В информационных системах и веб-сайтах государственного и частного сектора выявлено 816 уязвимостей.

Использование данных уязвимостей позволит злоумышленникам неправомерно получить удаленный доступ, удалять, редактировать и читать конфиденциальную информацию.

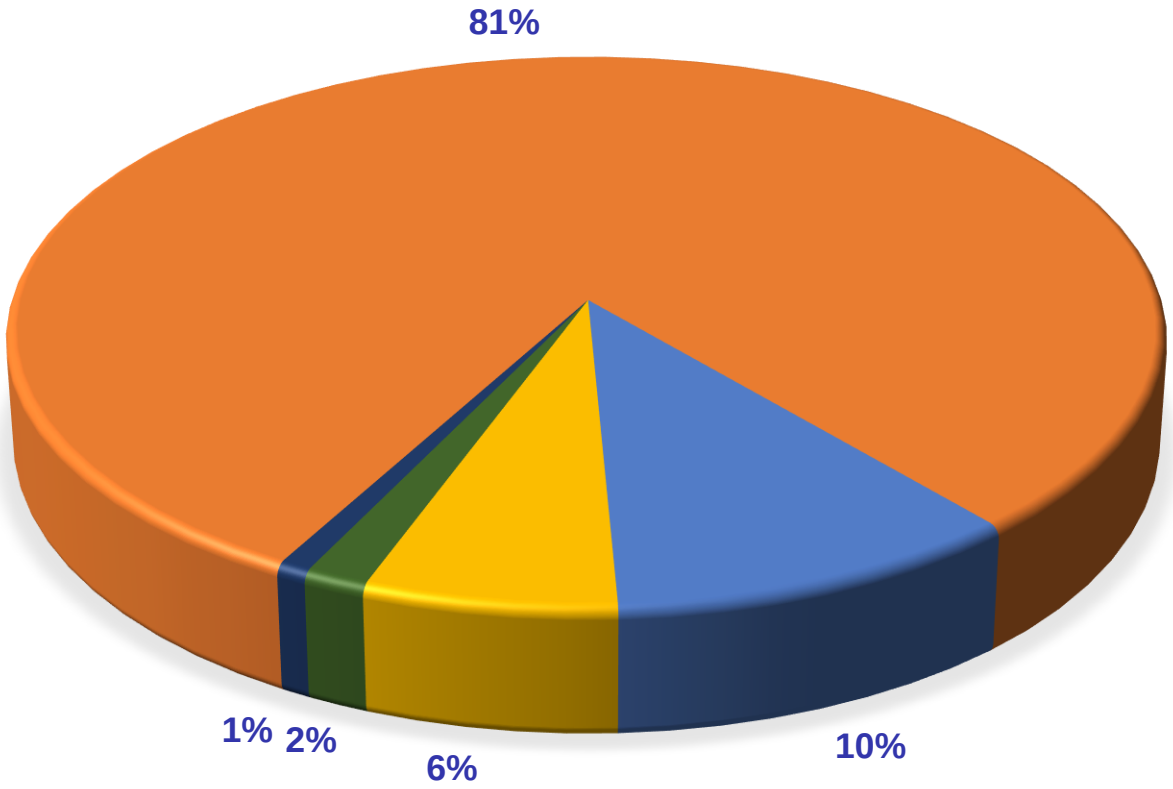
Угрозы кибербезопасности

Выявленные события кибербезопасности при мониторинге информационных систем государственных органов



Угрозы кибербезопасности

Выявленные угрозы кибербезопасности



- (106508) - относится к хостам ставшими участниками ботнет сетей;
- (3882) - связано с блокированием IP-адресов, попавших в чёрный список различных сервисов, по причине рассылки спам писем или перебора паролей;
- (8457) - использование TFTP-протокола (Trivial File Transfer Protocol) и связанных с ним портов (может привести к загрузки постороннего контента из-за отсутствия механизмов аутентификации);
- (2114) - использование уязвимого RDP протокола (Remote Desktop Protocol);
- (1042) - использовани программного обеспечения и СУБД, не имеющего механизма аутентификации, а также просроченные или имеющие недостоверную подпись SSL-сертификаты.

Международное сотрудничество

Активная деятельность по вступлению в ряды «FIRST.ORG» (в настоящее время является наблюдателем), сотрудничество и взаимодействие со службами CERT зарубежных стран в рамках двухсторонних меморандумов о сотрудничестве и взаимопонимании

Поддержание взаимодействия с сообществами, как ITU, OIC-CERT, PATC-ШОС, установление контактов с Индией, Японией, Малайзией, Республикой Корея, Объединенными Арабскими Эмиратами, Республикой Польша и другими странами

Участие в международных конференциях, семинарах по вопросам обеспечения информационной и кибербезопасности и борьбе с киберпреступностью

ITU
TF-CSIRT Trusted Introducer
OIC-CERT Computer Emergency Response Team
KZ-CERT
GEORGE C. MARSHALL EUROPEAN CENTER FOR SECURITY STUDIES
KISA Korea Internet & Security Agency
certin enhancing cyber security in India
JPCERT CC Japan Computer Emergency Response Team Coordination Center JPCERT コーディネーションセンター
CNCERT/CC 国家互联网应急中心
CERT.LV Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

НАПРАВЛЕНИЯ РАЗВИТИЯ

Разработка национальной стратегии кибербезопасности Республики Узбекистан

Разработка проекта Закона Республики Узбекистан «О кибербезопасности»

Подготовка квалифицированных кадров, а также повышение грамотности населения в сфере информационных технологий и обеспечения информационной безопасности,

Дальнейшее развитие международного сотрудничество в сфере обеспечения информационной безопасности

КОНТАКТЫ

Спасибо за внимание!

Республика Узбекистан,
100115, г. Ташкент, ул. Кирк киз, 10А

Телефон: +998712035511

E-mail: info@csec.uz, info@uzcert.uz
Веб-сайт: www.csec.uz , www.uzcert.uz